IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
NOTHERN DIVISION

NO. 2:18-CR-00037-1FL

UNITED STATES OF AMERICA	**:**	
	:	**SECOND**
VS	**:**	**MOTION TO SUPPRESS**
	:	
CHARLES ANTHONY WALKER	**:**	
DEFENDANT	**:**	

Now come the defendant by and through the undersigned attorney and moves the Court for an Order suppressing any and all evidence obtained as a result of two orders issued pursuant to 18 U.S.C. 2703(c) and (d). The first order was issued by North Carolina Superior Court Judge J. Carlton Cole in Pasquotank County on September 6, 2018. The second order was issued by North Carolina Superior Court Judge Bryan Collins in Wake County on October 18, 2018. Any information obtained as a result of either of these orders was obtained in violation of the Fourth Amendment of the United States Constitution. In support of this motion the undersigned shows unto the Court the following:

FACTS

1**.** On July 28, 2018, the Kay Jewelers in Elizabeth City, North Carolina was robbed at approximately 8:30 pm.

2. On October 11, 2018, the Kay Jewelers in Garner North Carolina Was robbed at approximately 4:00 p.m.

3. On September 6, 2018, K.M. Burgess a sworn officer of the Elizabeth City Police Department submitted to Superior Court Judge J. Carlton Cole an **APPLICATION FOR ORDER**

REQUIRING DICLOSURE OF HISTORICAL CELLULAR SITE INFORMATION. (See Attachment 1 which is attached hereto and incorporated herein as if set out herein verbatim)

4. This application asked for and Judge Cole ordered:

"1. That any and all providers of electronic service communications pursuant to Title 18 USC 2510(15), and any other provider of electronic communications as defined pursuant to N.C.G.S. 15A-286(9) or 18 U.S.C. 2519(15) shall provide to the Elizabeth City Police Department, with the assistance of the Federal Bureau of Investigation, any and all transactional records pertaining to cellular telephone calls, SMS texts, evolution data optimized (EVDO) information, per call measurement data (PCMD) and direct connect information, received by or transmitted from cellular towers, between **7:30 p.m. and 9:00 p.m. Eastern Standard Time on July 28 2018 or 11:30 p.m. and 1:00 a.m. Universal Time Coordinate, on July 28, 2018 through July 29, 2018,** that provide service in and around **3850 Conlon Way Elizabeth City NC 27909.** Also between **9:00 p.m. and 10:00 p.m. Eastern Standard Time on July 28, 2018 or 1:00 a.m. and 2:00 a.m. on July 29, 2018 Universal Time Coordinate** that provided service in and around **510 Virginia Rd, Edenton, NC 27932.**
2. The transactional records shall include; all transactional records (including, but not limited to; cell site information, call detail records for the interconnect, direct connect and dispatch service, SMS text records, data detail records and subscriber information, whether published or non-published) pertaining to any and all calls, data service, SMS texts, and direct connect calls, terminating or conducted through the above listed cell sites. In addition , the listed providers shall disclose cell site information relating to all numbers captured for ongoing, incoming and outgoing calls, and call data detail records with cell site and sector information from July 28, 2018 for all numbers captured for ongoing, incoming and outgoing calls upon oral or written request of Officers of the Elizabeth City Police Department, and/or the Federal Bureau of Investigation. Subscriber information includes but is not limited to name, address, other phone numbers, ESN/IMEI/IMSI/MIN/MSID/MEID or other specific identifiers for phone(s), other accounts, date of birth, social security number, other persons associated with the account, date of service initiation, date of deactivation, dates and changes to service, method of payment, payment method account numbers and financial entity, and entire account history, for all telephone service for the target telephone(s)/email, and all call, SMS, IP addresses, MAC addresses, EVDO, and PCMD detail records, including cell site location from.

5. Investigator Hunter Miller of the Garner Police Department submitted an almost identical application in Wake County on October 18, 2018 and Judge Collins entered an almost identical order as the order entered by Judge Cole. In fact, in paragraph 2 of the order the date of the Elizabeth City robbery appears. The only differences are the date and time of the offense, the

location of the robbery and the applicant. (See attachment 2 which is attached hereto and incorporated herein as if set out verbatim)

6. On November 19, 2018 a criminal complaint was issued charging the defendant and three co-defendants with the robbery of Kay Jewelers in Elizabeth City, North Carolina on July 28, 2018 in violation of 18 USC 1951 and 2. The criminal complaint relies heavily upon information received as a result of these court orders.

7. On December 4, 2018 the defendant and his three co-defendants were indicted in a five-count indictment. The defendant was charged with conspiracy to interfere with commerce by robbery and aiding and abetting, two counts of Hobbs Act robbery and brandishing a firearm in furtherance of a crime of violence.

8. Any and all evidence obtained as a result of either of the two orders entered pursuant to 18 USC 2703(c) and (d) was obtained in violation of the Fourth Amendment of the United States Constitution and should therefore be suppressed.

INTRODUCTION

The defendant, Charles Anthony Walker, moves this Court to suppress all historical cell phone records obtained by court order pursuant to18 U.S.C. § 2703(d). Because the use of a §2703(d) order to obtain cell tower data—a so-called "tower dump" order—is unconstitutional under the Fourth Amendment, the records, and all the fruits thereof, must be suppressed.

A tower dump order permits the government to collect the phone numbers and relative location (known as cell-site location information, or "CSLI") of all cellular device users within a particular radius. Not only did the government collect the phone numbers and locations of the phones; the government obtained an order to collect all information and data within the possession of the service providers. In addition to the defendant's phone number and location,

the tower dump here collected the information of numerous individuals within the range of the cell towers and from all service providers during the time frame requested in the orders. The facts of this case alone demonstrate why tower dump searches violate the Fourth Amendment. The orders themselves are overbroad and do not limit the information sought by the government. Because the information was used to identify the defendant's phone and its location the argument will focus on CSLI without giving up the right to challenge any other evidence obtained pursuant to the orders.

First, a request for a tower dump is a search under the Fourth Amendment. Collecting tower dump records violates cell phone users' reasonable expectation of privacy in their location data and in this case a broad range of information held by the service providers. It reveals their whereabouts, including their presence in constitutionally protected spaces, and permits the government to view more than would otherwise be publicly observable. CSLI, as collected via a tower dump, is a modern-day version of the "papers and effects" that the Framers chose to protect against "unreasonable searches and seizures." U.S. CONST. amend. IV. Moreover, the records at issue do not fall within the third-party doctrine, as cell-site location information is qualitatively different than a traditional business record, *see Carpenter v. United States*, 138 S. Ct. 2206, 2219–20 (2018) (noting the "revealing nature of CSLI"), and individuals do not "voluntarily convey this information to their cell phone providers, *see id.* at 2220 (stating that the rational of "voluntary exposure" does not "hold up when it comes to CSLI").

Second, a tower dump is specifically a *dragnet* search that is impermissible under the Fourth Amendment. *See United States v. Knotts*, 460 U.S. 282, 284 (1983). Tower dump records permit the government to "discover" a person "remotely and at will" without possessing any information about the individual's identity or phone number prior to the search. *Prince Jones v.*

United States, 168 A.3d 703, 713 (D.D.C. Sept. 21, 2017). Based on only a general timeframe and location, the government received the cell-site location records of numerous individuals in the hopes of finding one. The Court has never permitted such a sweeping search, with or without a warrant. This is for good reason: It is impossible to establish probable cause to search hundreds of individuals without a single named suspect. And it is impossible to meet the minimization and particularity requirements for a Fourth Amendment warrant for the same reason. As a result, tower dump orders are akin to the writs of assistance and general warrants that were so reviled by the Founding Fathers. *Riley v. California*, 134 S. Ct. 2473, 2494 (2014); *see also Carpenter* at 138 S. Ct. at 2267 (Gorsuch, J., dissenting) (questioning whether a tower dump might be "the *paradigmatic* example of 'too permeating police surveillance' and a dangerous tool of 'arbitrary' enforcement").

Although a tower dump can be a powerful tool for police in conducting criminal investigations, "police efficiency" cannot supersede the basic protections of the Fourth Amendment. *Riley*, 134 S. Ct. at 2493 (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971)) ("We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. . . . Privacy comes at a cost."). It should have been apparent to the government that a § 2703(d) order under the Stored Communications Act (SCA) provides insufficient judicial oversight over such an invasive search, and that even a warrant might be inadequate to meet the Fourth Amendment's warrant requirements of probable cause and particularity. The Fourth Amendment therefore requires suppression of the tower dump records.

BACKGROUND

Cell phones are a ubiquitous part of American life, with "396 million cell phone service accounts in the United States—for a Nation of 326 million people." *Carpenter*, 138 S. Ct. at

2211. These devices "faithfully follow [their] owners," *id.* at 2218, connecting to nearby cell sites "several times a minute whenever their signal is on, even if the owner is not using one of the phone's features." *Id.* at 2211. When a cell phone connects with a cell tower, it creates cell site location information (CSLI), which identifies a cell phone's approximate location. *Id.* In *Carpenter*, the Supreme Court held that individuals have a reasonable expectation of privacy in their physical movements. *Id.* at 2217.

As the number of cell phone users increase, so too does the number of cell sites. In addition to cell towers, cell sites can be found on "light posts, flagpoles, church steeples, or the sides of buildings." *Id.* at 2211. As companies such as Verizon and AT&T switch to more advanced wireless services to deliver "ultrafast downloads," these companies will install "hundreds of thousands" of additional cell towers. *See* Brian Fung, *The Future of 5G Mobile Data Could Hinge on a Battle over Utility Pole Fees*, Wash. Post, Sept. 24, 2018. This has and will continue to "lead to increasingly compact coverage areas, especially in urban areas." *Carpenter*, 138 S. Ct. at 2212. As a result, cell towers will be able to capture the CSLI of up to thousands of individuals at any given point in time, pinpointing their whereabouts with striking precision. *See id.* at 2218 ("Accordingly, when the government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.").

In this case, the government received an order for what is known as a cell tower dump under 18 U.S.C. § 2703(d) of the Stored Communications Act (SCA). A tower dump "pull[s] in the phone numbers and [proximate] location of everyone in the vicinity of the event." In other words, it provides the government with a record of every individual that was near a cell tower, or group of cell towers, during a given time period. These searches invade the privacy of not just one individual, but potentially thousands of people.

Smartphones connect to cell sites without users having to interact with the device at all. *See Carpenter*, 138 S. Ct. at 2220 ("[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up"). These connections occur as frequently as every seven seconds. Tower dump requests will therefore reveal increasingly large and precise amounts of location data as even more Americans switch to smartphones, and as improved technology permits cell phones to connect with towers at an even faster speed.

ARGUMENT

1. A Tower Dump Is a "Search" Under the Fourth Amendment.

The Supreme Court recently held in *Carpenter v. United States* that individuals have a reasonable expectation of privacy in their cell phone location data, and that the government's acquisition of those records from the defendant's cellular service provider was a Fourth Amendment search. 138 S. Ct. 2206, 2217 (2018). This holding must apply with equal force in the context of a tower dump request. Whether this Court applies the reasonable expectation of privacy framework set forth in *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring), or whether it employs a property-based theory of the Fourth Amendment, it should reach the same conclusion that tower dump is a search under the Fourth Amendment.

2. Users Have a Reasonable Expectation of Privacy in Their Cell Phone Location Data.

In considering whether citizens reasonably expect information to remain private, the Supreme Court has crafted "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361; *see also Carpenter*, 138 S. Ct. at

2213, 2217 (applying the *Katz* analysis in the context of CSLI and concluding that users have a reasonable expectation of privacy in this information). For reasons discussed below, the defendant has evinced both a subjective and objective expectation of privacy, and therefore a tower dump is a Fourth Amendment search.

Although the Court did not rule on the constitutionality of tower dumps in *Carpenter*, 138 S. Ct. at 2220, the Court's rationales for concluding that users have a reasonable expectation of privacy in their long-term CSLI apply equally to the CSLI received from a tower dump. In *Carpenter*, the Court explained that "the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection" give rise to a reasonable expectation of privacy. *Id.* at 2223. These factors are just as relevant when the government collects CSLI through a tower dump, and they demand at least the same degree of Fourth Amendment protection. This is especially true given the unique First Amendment concerns raised by tower dump orders.

In addition, the third-party doctrine does not apply to cell phone location information collected during a tower dump. In *Carpenter*, the Court held that the third-party doctrine could not apply to cell-site location information because "the nature of the particular documents sought" were highly "revealing" and because users did not "voluntarily" share that information with the third-party. *See Carpenter* at 2219–20. The cell-site location information collected pursuant to a tower dump is similar in both respects.

3. A Tower Dump Collects Information that is "Deeply Revealing" Because It Intrudes on Constitutionally Protected Spaces and Activities.

Tower dumps reveal information about constitutionally protected spaces such as the home—which is "presumptively unreasonable in the absence of a search warrant." *Katz*, 389 U.S. at 361. Cell phone location data is precise; it can be used to locate someone "not only

around town but also within a particular building." *Riley*, 134 S. Ct. at 2490. A tower dump will provide a time stamped CSLI of the device wherever the user carried it. Because "individuals . . . compulsively carry cell phones with them all the time," *Carpenter*, 138 S. Ct. at 2218, users will carry their devices with them within their homes. Because a tower dump gathers the CSLI of multiple users—up to thousands—at a time, the risk that a tower dump will reveal the precise location information of a at least one individual within her home is high. The Court has repeatedly emphasized that "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion" is at the very heart of the Fourth Amendment. *Silverman v. United States*, 365 U.S. 505, 511 (1961); *Kyllo v. United States*, 533 U.S. 27, 37 (2001); *Knotts*, 460 U.S. at 282 ; *United States v. Karo*, 468 U.S. 705, 715 (1984). The sanctity of the home was assured at the time of the adoption of the Fourth Amendment, and the Court has long expressed concern with establishing "what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 34. A tower dump is far too expansive an invasion of the "sanctity of the home" or any other constitutionally protected area. *Id.* at 37.

Cell phone information gleaned from a tower dump can also reveal private facts about protected activities and other intimate spaces, violating an individual's reasonable expectation of privacy in a way that raises unique First Amendment concerns. And as the Supreme Court has repeatedly emphasized, courts must be careful to apply Fourth Amendment requirements with "the most scrupulous exactitude" when they implicate First Amendment concerns. *Stanford v. Texas*, 379 U.S. 476, 485 (1965) ("leaving the protection of [First Amendment] freedoms to the whim of the officers charged with executing the warrant" is unconstitutional); *see also Marcus v. Search Warrant of Property*, 367 U.S. 717, 729 (1961) (finding that additional safeguards were

needed to protect freedom of speech when officers searched books under an overbroad warrant). Tower dumps reveal all cell phone users within a certain area, and as such, they may reveal sensitive associations and activities, that implicate First Amendment concerns no less than the "records, pamphlets, [and] … lists" in *Stanford*. 379 U.S. at 486. This is especially true in this case because of the overbroad and expansive nature of the application and each order issued.

In *Carpenter*, the Court acknowledged this potential, noting: "A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." 138 S. Ct. at 2218. As one *amicus* brief in *Carpenter* noted, a tower dump of a cell site near an 8:30 pm Alcoholics Anonymous meeting "will reveal all the devices—and therefore individuals—in that meeting. . . . The same conclusions hold for other sensitive and protected associational activities—including religious evangelism, student activism, and union organizing." *Brief of Technology Experts as Amici Curiae in Support of Petitioner* at 35-36, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402), 2017 WL 3530967, at *54. Another *amicus* brief in *Carpenter* observed that *"*[d]ue to the ubiquitous nature of cell phones, location information gleaned from cell towers can disclose an individual's expressive and associational activities such as "a journalist's newsgathering process." *Brief of The Reporters Committee for Freedom of the Press and 19 Media Organizations as Amici Curiae in Support of Petitioner* at 10, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402), 2017 WL 3530966, at *14. These briefs expressed fears that CSLI can reveal information not only about intimate and constitutionally protected spaces, but also infringe on First Amendment activities. *See United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms"). By revealing information about constitutionally

protected spaces and protected activities, tower dumps have precisely the pernicious effect on an individual's realm of privacy that the Court has held violates the Fourth Amendment. *See, e.g.*, *Kyllo*, 533 U.S. at 40.

4. Tower Dumps Provide the Government Unprecedented Powers of Surveillance that Upset Traditional Expectations of Privacy.

In a series of cases addressing the power of "technology [to] enhance[] the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," the Supreme Court "has sought to 'assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo*, 533 U.S. at 34) (last alteration in original); *accord Jones*, 565 U.S. at 406. As Justice Alito explained in *Jones*, "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical." 565 U.S. at 429 (Alito, J., concurring in judgment). Accordingly, the Court has remained vigilant "to ensure that the 'progress of science' does not erode Fourth Amendment protections." *Carpenter*, 138 S. Ct. at 2223.

Thus, the Supreme Court has held that police must obtain a warrant before using a thermal imager to observe details about the interior of a home that, prior to the availability of the technology, would have been shielded from view as a practical matter. *Kyllo*, 533 U.S. at 35. Likewise, a warrant is required to search the contents of a phone seized incident to arrest because the traditional rule permitting warrantless searches incident to arrest fails to "strike the appropriate balance" given the "immense storage capacity" of modern cell phones. *Riley*, 134 S. Ct. at 2484, 2489.

Like the historical CSLI in *Carpenter*, a tower dump is a virtual time machine with the power to quickly and easily locate people at any point in the past – a power unknown to the government until very recently. While one may not reasonably expect to remain unobserved on

public roads, *Knotts,* 460 U.S. 276, 281 (1983), the *Carpenter* Court was careful to note that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere." 138 S. Ct. at 2217. Instead, the *Carpenter* majority observed that, unlike the real-time honing beeper used in *Knotts,* "the retrospective quality of the data here gives police access to a category of information otherwise unknowable." *Id.* at 2218. Indeed, "with access to CSLI, the government can now travel back in time to retrace a person's whereabouts." *Id.*

This retrospective quality distinguishes tower dumps from the real-time tracking in *Knotts*, which "amounted principally to the following of an automobile on public streets and highways." 460 U.S. at 281; *see also Prince Jones*, 168 A.3d at 712 (citing *Knotts*, 460 U.S. at 282) ("at their core these devices merely enable police officers to accomplish the same task that they could have accomplished through '[v]isual surveillance from public places.'"). Indeed, tower dumps allow the government to track not just one person, but thousands of people – all at once, and over any interval in the past. They also enable the government to do so at little cost, digitally reconstructing a picture of almost everyone who was in a given location at a given time.

Access to historical CSLI is "remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense." *Carpenter*, 138 S. Ct. at 2217–18. Whereas, "[i]n the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection[, w]ith access to CSLI, the Government can now travel back in time" to retrace the whereabouts of thousands of people. *Id.* at 2218.

The government has never had such comprehensive surveillance abilities, and a §2703(d) order should not be the only barrier to such omnipotent surveillance. As the Supreme Court

reiterated in *Carpenter*, the very purpose of the Fourth Amendment is to secure "the privacies of life" against "arbitrary power," and "to place obstacles in the way of a too permeating police surveillance." 138 S. Ct. at 2214. Given their ability to reconstruct the comings and goings of entire communities, reveal sensitive and constitutionally-protected information and activities – and to do so cheapy and easily, warrantless tower dumps upend the balance crafted by the Framers and violate the Fourth Amendment.

5. The Third-Party Doctrine Does Not Apply to Data Collected by a Tower Dump Because the Collection of CSLI is Inescapable and Automatic.

The *Carpenter* Court squarely rejected applying the third-party doctrine to CSLI. The Court provided two main rationales for this decision: (1) that CSLI is particularly revealing in nature and qualitatively different from types of business records to which the doctrine may apply, and (2) that users do not voluntarily share their cell-site location information. *See id.* at 2219–20. These two rationales apply with equal force to a tower dump search.

Cell-site records are qualitatively different from the business records to which the third-party doctrine traditionally applies. *See Smith v. Maryland*, 442 U.S. 735, 742 (phone numbers dialed on a landline); *United States v. Miller*, 425 U.S. 435, 440 (1976) (bank statements and deposit slips). Although tower dumps similarly concern the government's collection of telephone numbers, the records here are very different from the records collected by the pen register used in *Smith. See Carpenter,* 138 S. Ct. at 2219 (contrasting CSLI with "the limited capabilities of a pen register").

First, *Smith* involved a "one-time, targeted request for data regarding an individual suspect in a criminal investigation." *Klayman v. Obama*, 957 F. Supp. 2d 1, 33 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015). A tower dump, in comparison, is neither a targeted search nor a narrow search of one individual. Instead, it is a dragnet cast by law

enforcement because they cannot identify a suspect, implicating hundreds or thousands of innocent individuals in the process.

Second, a pen register reveals only the telephone numbers that an individual dialed. *Carpenter*, 138 S. Ct. at 2216 (citing *Smith*, 442 U.S. at 742)). In comparison, a tower dump reveals not only a chronological list of telephone numbers, but also the cell phone's approximate location. Location information can provide a wealth of "identifying information," *Riley*, 134 S. Ct. at 2493, if, for example, a cell tower is located near a church, doctor's office, or political headquarters.

Individuals do not voluntarily share their location information with their cell-phone provider, further supporting the notion that third-party doctrine is inapposite in this context. The third-party doctrine rests on the assumption that an individual cannot reasonably expect "information he voluntarily turns over to third parties" to remain private. *Smith*, 442 U.S. at 44. But as in *Carpenter*, cell phone users do not "share" their location data with service providers on a voluntary basis: "Cell phone location information is not truly 'shared' as one normally understands the term. In the first place, cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." 138 S. Ct. at 2220 (quoting *Riley*, 134 S. Ct. at 2484). Moreover, "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up." *Carpenter*, 138 S. Ct. at 2220. The only way an individual could avoid "sharing" their cell phone location data would be to "disconnect the phone from the network" altogether, rendering it useless as a communication device. *Id.* It cannot be that by choosing to "participat[e] in modern society" and merely carrying a cell phone which is switched on, an individual relinquishes any expectation of privacy in their location information. *Id.*

6. CSLI is Property That Is Protected by the Fourth Amendment's Prohibition Against Unreasonable Searches and Seizures.

Under a property-based theory of the Fourth Amendment, defendant's location data constitutes [his/her] "papers or effects," whether or not they are held by a third-party cell phone provider, and thus cannot be searched or seized without a warrant. *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting). In his opinion in *Carpenter*, Justice Gorsuch argued that under a "traditional approach" to the Fourth Amendment, the protection against unreasonable searches and seizures applied as long as "a house, paper or effect was yours under law." *Id.* at 2267–68 (Gorsuch, J., dissenting); *see also Florida v. Jardines*, 569 U.S. 1, 5 (2013) (citing *United States v. Jones*, 565 U.S. 400, 406 n.3 (2012)) ("The Amendment establishes a simple baseline, one that for much of our history formed the exclusive basis for its protections: When 'the Government obtains information by physically intruding' on persons, houses, papers, or effects, 'a search' within the original meaning of the Fourth Amendment 'undoubtedly occurred'"). Justice Gorsuch drew a strong analogy to mailed letters, in which people have had an established Fourth Amendment property interests for over a century, whether or not these letters are held by the post office. *Id.* at 2269 (citing *Ex parte Jackson*, 96 U.S. 727, 733 (1877)). Just as individuals retain property interests in letters in transit while the letters are in the physical possession of a post office, cell phone users have property interests in their location data even when it is stored by cell phone service providers. As Justice Gorsuch explained, private and sensitive records in the hands of a third party can fall under the Fourth Amendment's protection of a person's "papers" even when control of and proprietary interest in those records is divided between the individual to whom they pertain (i.e., the Defendant) and the business with custody of them (i.e., the cellular service provider). 138 S. Ct. at 2268–69.

Where "positive law" allocates at least some property rights in third-party-held data to an individual, the Fourth Amendment's protections apply. *Id.* at 2270. Here, cell phone location information is specifically protected by law. The Federal Telecommunications Act requires "express prior authorization" of the customer before a service provider can "use or disclose . . . call location information," which the law categorizes as "customer proprietary information." 47 U.S.C. § 222(f). The statute therefore grants users substantial legal interests in this information, including at least some right to include, exclude, and control its use." *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting). If location data generated by a cell phone constitutes the user's property, then its seizure and search by the government without a warrant violates the Fourth Amendment. *See also Riley*, 134 S. Ct. 2473, 2490 (holding Fourth Amendment applies to information contained on a cell phone *and* associated information "stored on remote servers" since "[c]ell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.").

7. A Tower Dump Is a Dragnet Search Forbidden by the Fourth Amendment Because It is Akin to a General Warrant.

Tower dumps are the epitome of the "dragnet-type law enforcement practice" that the Court feared in *Knotts*, 460 U.S. at 284, sweeping up the location data of up to thousands of innocent individuals in the hopes of finding one potential lead. The Court has always been "careful to distinguish between rudimentary tracking . . . and more sweeping modes of surveillance," in deciding whether a search is entitled to heightened protection under the Fourth Amendment. *Carpenter*, 138 S. Ct. at 2215 (citing *Knotts*, 460 U.S. at 284), and tower dumps fall on the "sweeping" end of this spectrum.

A comparison to the "rudimentary tracking" in beeper cases such as *Knotts* and *Karo* illuminates the drastically different dragnet nature of a tower dump. In the beeper cases, the

government only sought to track *one* individual. To do so, law enforcement first needed to identify the individual, and then to physically install a tracking device on an object that was in their possession. With a tower dump, however, the government no longer needs identify a suspect. Instead, "[w]ith just the click of a button, the government can access each carrier's deep repository of historical location information at practically no expense." *Carpenter*, 138 S. Ct. at 2218; *see also United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) ("Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive").

Tower dump information can be even more invasive than a single individual's historical CSLI, posing a heightened threat to privacy. A tower dump near "the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, [or] the gay bar" can allow the government to piece together a comprehensive overview of *every* attendee in such a space. *Jones*, 565 U.S. at 415 (Sotomayor, J. concurring) (quoting *People v.* Weaver, 909 N.E.2d 1195, 1999 (N.Y. 2009)). While the Court has already expressed concern about creating a "comprehensive record of a person's public movements," *Riley* 134 S. Ct. at 2490 (citing *Jones*, 565 U.S. at 415), a tower dump raises a corollary concern—creating a comprehensive record of all individuals at a given location. At issue is not only the government's ability to "ascertain, more or less at will, [an individual's] political and religious beliefs, sexual habits, and so on," Jones, 565 U.S. at 416 (Sotomayor, J., concurring); it is their ability to do so for hundreds or thousands of individuals all at once.

The dragnet nature of the search is further evident from the fact that the government may keep the data for future use. The government may have access to "the most advanced twenty-first

century tools, allowing it to 'store such records and efficiently mine them for information years into the future,'" and creating a risk of repeated surveillance. *Klayman*, 957 F. Supp. 2d at 33 (citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)); *see also Comprehensive Drug Testing*, 621 F.3d 1162, 1175 (9th Cir. 2010) (en banc) (per curiam) (remarking that "the threat to the privacy of innocent parties from a vigorous criminal investigation" is heightened when sensitive data of multiple individuals is intermingled in electronic storage.). The Supreme Court is already concerned about the potential for abuse in tracking one person's location. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) ("the Government's unconstrained power to assemble data that reveal private aspects of identity is susceptible to abuse"). Tower dumps only compound that fear by capturing the location data of hundreds or thousands of people at once. Based on its capacity to reveal sensitive information about countless individuals, a tower dump is the hallmark of a "dragnet search." *See Carpenter*, 138 S. Ct. at 2267 (Gorsuch, J., dissenting).

A tower dump is the modern-day equivalent of searching every home in a several-block radius of a reported gunshot or searching the bags of every person walking along Broadway because of a theft in Times Square. Without the name or number of a single suspect, law enforcement invades the privacy of hundreds or thousands of individuals, just because they were in the area. *Cf. Sibron v. New York*, 392 U.S. 40, 63–64 (1968) (holding that "[t]he suspect's mere act of talking with a number of known narcotics addicts over an eight-hour period" did not give rise to neither reasonable suspicion nor probable cause to search him). Tower dumps harken back to the reviled general warrants and "writs of assistance" that permitted "British officers to rummage through homes in an unrestrained search for evidence of criminal activity;" searches that "helped spark the Revolution itself." *Riley*, 134 S. Ct. at 2494; *Carpenter*, 138 S. Ct. at 2213 (citing *Riley*, 134 S. Ct. at 2494). This type of "exploratory rummaging" is forbidden by the

Fourth Amendment. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). *See also Wilkes v. Wood*, 98 Eng. Rep. 489, 498 (1763) (condemning a search where the "discretionary power [was] given to messengers to search wherever their suspicions may chance to fall"); *Grumon v. Raymond*, 1 Conn. 40, 43 (1814) (holding that a "warrant to search all suspected places [for stolen goods]" was unlawful because "every citizen of the United States within the jurisdiction of the justice to try for theft, was liable to be arrested").

Moreover, tower dumps are not subject to the same practical constraints of previous eras, *cf. Riley*, 134 S. Ct. at 2494, in which "limited police resources and community hostility" served as a check on government behavior. *Illinois v. Lidster*, 540 U.S. 419, 426 (2004). With tower dumps, individuals will not be alerted when law enforcement officials obtain their CSLI, *see* Owsley, 16 U. Pa. J. Const. L. at 46, and the government can do so at little to no cost. *See Carpenter*, 138 S. Ct. at 2218 (noting that the government can access "historical location information at practically no expense"). This makes a tower dump all the more dangerous and risks "alter[ing] the relationship between citizen and government in a way that is inimical to democratic society." *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

Finally, the increasing use of tower dumps at the initial stages of an investigation further amplifies these concerns. Although "the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities," a tower dump also "risks Government encroaching of the sort the Framers, 'after consulting the lessons of history,' drafted the Fourth Amendment to prevent." *Carpenter*, 138 S. Ct. at 2223.

8. A Tower Dump is an Unconstitutional Search Under the Fourth Amendment and Suppression of the Tower Dump Records Is Required.

Tower dumps pose obvious privacy risks by scooping up the CSLI of anyone and everyone in the vicinity of a suspected crime. They are impermissible general warrants that

violate the Fourth Amendment. Indeed, it is likely impossible to establish probable cause to search and seize the CSLI of hundreds or thousands of people without even a single named suspect. As such, this Court should hold that the government's use of the tower dump records is unconstitutional under the Fourth Amendment and suppress the data obtained.

Tower dumps are wholly incompatible with the Fourth Amendment. It is probably impossible to establish enough probable cause necessary to search the CSLI of everyone in a given vicinity. *See Ybarra v. Illinois*, 444 U.S. 85, 86 (1979) (noting that "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person."). And for the same reason, the government will also be unable to "particularly describe the 'things to be seized." *Dalia v. United States*, 441 U.S. 238, 255 (1979) (citing *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). Although the government might be able identify the place to be searched in advance of a tower dump request, it cannot state with particularity the individuals it is searching—let alone the name of a single targeted individual or phone number. *See, e.g.*, *Groh v. Ramirez*, 540 U.S. 551, 558 (2004) (noting that the warrant lacked particularity because the warrant "did not describe the items to be seized *at all*"); *see also United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (noting that there is a "heightened sensitivity to the particularity requirement in the context of digital searches."). The inability to follow the probable cause and particularity requirements is even more alarming where, as here, the data to be seized raises significant First Amendment concerns. *See Stanford*, 379 U.S. at 485. The consequence of the inability to apply these criteria to a tower dump is simple: a warrant cannot authorize one.

Assuming *arguendo* that a tower dump is not categorically unconstitutional, then a carefully tailored warrant supported by probable cause would be the only way to authorize such a

drastic measure. The rationale of *Carpenter* makes that much clear. *Carpenter*, 138 S. Ct. at 2221. Moreover, when a search has the potential to sweep up information that does not pertain to the suspect under investigation, courts must ensure that the government has taken steps to ensure minimization and particularity of the search. A warrant for tower-dump data could only be valid if—at a minimum—it requires minimization of the amount of innocent third parties' data collected, restricts retention of such data after the search, and mandates notice to all persons whose cell phone location information the government has obtained.

Here, instead of a warrant, the government used a § 2703(d) order, which requires only "specific and articulable facts showing that there are reasonable grounds" for believing that the records are "relevant and material to an ongoing investigation." 18 U.S.C. § 2703(d). As the *Carpenter* majority explained, "[t]hat showing falls well short of the probable cause required for a warrant" and allowing it would be a "'gigantic' departure from the probable cause rule." 138 S. Ct. at 2210; *see also Owsley Opinion I*, 930 F. Supp. 2d at 702 (explaining that the "failure to address the privacy rights for the Fourth Amendment concerns of . . . innocent subscribers whose information will be compromised at a request of the cell tower dump is another factor warranting the denial" of § 2703(d) order). The government's failure to get a probable cause warrant that complies with the Fourth Amendment's particularity and notice requirements renders the search unconstitutional. Consequently, this Court should suppress the tower dump records, as well as any fruits thereof. *See Wong Sun v. United States*, 371 U.S. 484-488 (1963).

9. Because the Stored Communications Act Does Not Authorize Tower Dumps, the Good-Faith Exception to the Exclusionary Rule Does Not Apply.

The good-faith exception does not apply when the government relies on a statute that does not authorize the Fourth Amendment search. *Illinois v. Krull*, 480 U.S. 340, 360 n.17 (1987) (declining to apply good faith exception "when police officers act outside the scope of the

statute, albeit in good faith). Here, the government relies on the Stored Communications Act, which does not authorize tower dump orders. As a result, any reliance on the SCA was objectively unreasonable. *See Krull*, 480 U.S. at 355 (adopting an objective standard for reasonableness of good faith reliance on statute). The good faith exception thus does not apply to the CSLI obtained in this case.

A. The Text of the SCA Does Not Authorize This Type of Search.

First, the SCA imposes a general prohibition on government access to customer records held by cell service providers, subject only to enumerated exceptions. One of those exceptions permits the government to obtain a warrant or court order for records pertaining to "a subscriber to or customer of" the provider. 18 U.S.C. § 2703(c)(1). Because this congressional authorization is phrased in the singular, there is a serious textual question as to whether the SCA permits tower dumps at all, since they inescapably involve the records of large numbers of people.

The SCA also prohibits the government from obtaining records that are not "relevant and material" to the ongoing criminal investigation. *See* 18 U.S.C. § 2703(d). At minimum, the "relevant and material" requirement under the SCA is more demanding than the mere "relevance" standard governing the issuance of administrative and grand-jury subpoenas. Under the lower "relevance" standard, courts have consistently required that the particular records demanded by the government have an actual connection to a particular investigation. *See, e.g.*, *Bowman Dairy Co. v. United States*, 341 U.S. 214, 221 (1951) (invalidating a subpoena's "catch-all provision" on the grounds that it was "merely a fishing expedition to see what may turn up"). Courts have also rejected or narrowed subpoenas that, because they fail to identify the outer bounds of the categories of records they seek, cover large volumes of *irrelevant* documents. *See In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993*, 846 F. Supp. 11, 12 (S.D.N.Y.

1994) (Mukasey, J.) (quashing a grand-jury subpoena that demanded the entire contents of "computer hard drives and floppy disks," because the materials "contain[ed] some data concededly irrelevant to the grand jury inquiry").

Where, as here, the government indiscriminately seeks records implicating the privacy of hundreds or thousands of individuals in one fell swoop, it cannot possibly meet the standard in establishing a "relevant and material" need for *all* of these records. At best, the government is seeking records from individuals who may share a cellular service provider with a potential, unknown criminal suspect. That is plainly not the kind of search authorized by the SCA.

B. The Government Knew that Cell Tower Searches Raise Heightened Privacy Concerns that at Minimum Require a Warrant.

The government should have known that only a warrant could possibly protect against an unreasonable invasion of privacy. There is no way to conceptualize a tower dump search as anything but a Fourth Amendment search, clearly requiring some level of judicial oversight beyond a § 2703(d) order. This is especially true following *Carpenter*, which held that law enforcement seeking to obtain CSLI must, at minimum, obtain a warrant based on probable cause: "[A]n order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records." 138 S. Ct. at 2210–11. Before compelling a wireless carrier to turn over a subscriber's CSLI, the government's obligation is a familiar one—get a warrant." *Id.* at 2221; *see also Riley*, 134 S. Ct. at 2495. The holding in *Carpenter* strengthens the conclusion that the SCA does not authorize this acquisition of defendant's cell site location via a tower dump request, that a heightened form of judicial oversight was required, and that the good faith exception to the exclusionary rule should not apply.

CONCLUSION

For the foregoing reasons, Charles Anthony Walker respectfully requests that this Court suppress the tower dump records and all evidence obtained as a result thereof and grant such further relief as it deems appropriate.

Respectfully submitted this 12th day of June 2020.

H.P. WILLIAMS, JR., PLLC

BY: /s/ H.P. Williams, Jr.
H.P. WILLIAMS, JR.
APPOINTED ATTORNEY FOR
DEFENDANT: CHARLES ANTHONY WALKER
STATE BAR NO. 8566
408 E. COLONIAL AVE, SUITE B
ELIZABETH CITY, NC 27909
TELEPHONE: 252-337-4518
hpw@hpwilliamslaw.com

CERTIFICATE OF SERVICE

This is to certify that a copy of the foregoing was served upon:

Daniel W. Smith and
Robert J. Dodson
Assistant U.S. Attorney
Criminal Division
Eastern District of North Carolina
150 Fayetteville St. Suite 2100
Raleigh, North Carolina 27601

By electronically filing the foregoing with the Clerk on June 12, 2020 using the CM/ECF system which will send notification of such filing to the above.

This the 12th day of June 2020.

/s/ H.P. Williams, Jr.
H.P. WILLIAMS, JR., ATTORNEY
FOR DEFENDANT